

View f:\emailobj\200503\7\331151558.txt

Page 1 of 4

View f:\emailobj\200503\7\331151558.txt

From: jeffg@jeffg.org  
Date: 3/31/2005 3:14:32 PM  
To: webmail@chambliss-iq.senate.gov  
Subject: State Department Electronic Passport Proposal

---

Marietta, Georgia  
31 March 2005

To  
Chief, Legal Division  
Office of Passport Policy, Planning, and Advisory Services

In regards to  
RIN 1400-AB93, Public Notice 4993  
Electronic Passport  
AGENCY: Department of State.  
ACTION: Proposed rule.  
As published in  
Federal Register: February 18, 2005 (Volume 70, Number 33)

Dear Sir or Madam:

I am writing to express my disagreement with the State Department's proposal to incorporate Radio Frequency Identification (RFID) technology in future passports issued by the United States. While I applaud the effort to modernize travel documents, I have serious concerns regarding the choice of RFID for this application. Foremost is the prospect of thieves, kidnappers, or terrorists exploiting the chosen technology to cull American citizens out of crowds by remotely activating and reading the RFID chip. Secondary is concern over invasion of privacy and identity theft.

To quote the public notice:

"Although surreptitiously activating the electronic chip remotely and then reading the return signal amid ambient electronic noise is considered technically very difficult, the Department is taking measures to prevent skimming of the unencrypted data. By the time the first electronic passport is issued, the Department intends to place an anti-skimming feature in the passport."

Regarding this paragraph, I would counter that technical difficulty is notoriously unreliable as a barrier to the commission of criminal acts. If the Department expects a promise of an "anti-skimming feature" to ease such concerns, it should discuss such a feature in detail and extend the period for public comment.

Quoting again:

"Eavesdropping can only occur while the electronic chip is being read using a specially designed reader furnished with the proper public key. Eavesdropping is difficult to achieve, however, in a secured port of entry environment. In such an environment, the equipment needed to

View f:\emailobj\200503\7\331151558.txt

Page 2 of 4

eavesdrop would be obvious and detectable to authorities managing the port of entry. The State Department will work vigorously with other governments to encourage them to eliminate the threat of eavesdropping by requiring all chip readers to be electronically shielded to prevent signals from being transmitted beyond the reader."

These statements fail to take into account any hitherto undiscovered vulnerabilities in the technologies proposed for this application. The necessary readers will inevitably become available on the open, gray, or black markets. Public keys can themselves be discovered by eavesdropping. Furthermore, since the Department intends for chip readers to be electronically shielded, it is implied that the passport bearer or border agent would need to place the passport into an enclosure of some kind. With this requirement, the benefits of using RFID disappear almost completely -- as long as I (or an agent) must place my passport in a receptacle, why not require physical contact or line-of-sight between that receptacle and the document? Technologies such as contact-based smart cards and two-dimensional barcodes exist today that meet these requirements and suffer from none of the security and privacy concerns outlined above.

In conclusion, the proposal to use RFID as a part of a future electronic passport document seems ill-considered and fraught with risks that clearly outweigh its potential benefits. I urge the State Department to withdraw this proposal in its current form and to reissue it with its RFID component replaced with a different technology that requires either physical contact or optical scanning.

Best Regards,  
Jeffrey Gehlbach  
357 Cherokee Street  
Marietta, GA  
(404) 214-6014

Copies via electronic mail and fax to:  
Representative Phil Gingrey (GA-11)  
Senator Johnny Isakson (GA)  
Senator Saxby Chambliss (GA)

==== Original Formatted Message Starts Here -====

Sender's IP address = 209.101.206.193  
<APP>SCCMAIL  
<PREFIX>Mr.</PREFIX>  
<FIRST>Jeffrey</FIRST>  
<LAST>Gehlbach</LAST>  
<ADDR1>357 Cherokee St</ADDR1>  
<ADDR2></ADDR2>  
<CITY>Marietta</CITY>  
<STATE>GA</STATE>  
<ZIP>30060</ZIP>  
<PHONE>404-214-6014</PHONE>  
<EMAIL>jeffg@jeffg.org</EMAIL>  
<ISSUE>hmlid</ISSUE>  
<AFFL>reply</AFFL>  
<MSG>Marietta, Georgia  
31 March 2005

To  
Chief, Legal Division

**Burrows, Dan**

**From:** Web forms [webforms@www6a.house.gov]  
**Sent:** Monday, March 28, 2005 5:05 PM  
**To:** Wolf, Write  
**Subject:** E-mail to Congressman Wolf

-----  
Date: 03/28/2005

Time: 16:49

Web page used to link to the form:

[http://www.house.gov/htbin/formproc\\_zs/wolf/zip\\_authen.txt&form=/wolf/message.html](http://www.house.gov/htbin/formproc_zs/wolf/zip_authen.txt&form=/wolf/message.html)

Web Browser: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

IP address: 69.161.29.132  
-----

Salutation: Mr.

Name: Richard Will

Address: 7276 King William St.

Address 2:

City: Warrenton

20187 - 4412

State: Virginia

Phone: (540)349-1787

E-mail: rwill@coordgrp.com  
-----

Message:

-----  
Congressman Wolf,

In the decades you have well represented my family and me, I've had only one other activity I've needed to call to your attention. The abstract below, if accurate, suggests a well-meaning but misguided attempt by the Government to protect its citizens. I believe it requires a careful look. Thanks for your continuing hard work.

=====

The State Department is proposing to embed an RFID chip into every American passport. It would contain personal details - name, date of birth, passport number, and even a digital picture, and can be read by anyone reasonably close with an RFID chip reader.

Anyone from petty thieves and pickpockets, up to identity thieves, kidnappers and terrorists would love to know who in a crowd is an American foreigner and therefore an easy victim. Another way to abuse this information is to just hang out at an airport and get the details of departing passengers - their houses may be unattended and good choices to burgle.

The State Department acknowledges some risks but says in response that to 'skim' this information is technically very difficult. Some scientists apparently vehemently disagree. A State Department spokesperson is supposed to have said these chips can only be read from 4" away. But there is one device on the market for \$300 that can read RFID chips from 450 ft.

The State Department has also suggested people could wrap their passports in tinfoil to insulate them from people with unauthorized readers!!!

The State Department is accepting comments on this proposed change to our passports through next Monday (April 4).

1240507

**Grassley, Chuck (Grassley)**

---

**From:** Pham Dieu-Le T [PhamDieu-LeT@JohnDeere.com]  
**Sent:** Tuesday, March 29, 2005 9:54 AM  
**To:** PassportRules@State.Gov  
**Cc:** Grassley, Chuck (Grassley)  
**Subject:** New type of passport

Chief, Legal Division,

I am totally against this newly "design" passport. As an Computer Analyst for 30 years and a 22 years old child, I can vouch that anyone of us could break the code if we put all our energy into this task regardless of how the information is stored!

I do not wish to have somebody at the airport read my very personal file using the device on the market today from 450ft! Like the Sate Department would also suggested that people should wrap their passport with tinfoil to avoid unauthorized readers! If this is the case why do you even want to put my personal information out there for people to read?

I hope the State Department employs the best of the best IT Analysts to know better that this kind of coding could be broken, stolen, read, etc... by anybody!

Your consideration to the people would be very much appreciated.

Regards,

Pham

Diêu-Lê Pham  
1925 Burr Oak Pl  
Bettendorf, IA. 52722  
Infrastructure Analyst  
phamdieu-let@johndeere.com  
(309) 765-4067  
(309) 765-5168 (Fax)  
(309) 781-6490 (Cell)  
1-877-330-1632 (Pager)